THE EMBODIMENTS OF THE INVENTION IN WHICH AN EXCLUSIVE PROPERTY OR PRIVILEGE IS CLAIMED ARE DEFINED AS FOLLOWS:

1. The method for providing cryptographic functions to data packets at the PPP layer of a network stack, the method including the steps of:

intercepting PPP datagrams inbound to said network stack and outbound of network stack, said PPP datagrams having at least one encapsulated data packet en route along the protocol stack;

decapsulating said PPP datagrams to retrieve said at least one encapsulated data packet;

determining whether to process said at least one data packet by examining said data packet;

modifying said data packet to provide said cryptographic functions; and

encapsulating said at least one data packet for transmission to a next layer of said network stack.

2. The method of claim 1 wherein said data packet is an IP packet having a header, an address and data.

3. The method of claim 1 wherein said step of modifying said data packet includes the further step of selecting an IPSec protocol.

4. The method of claim 1 wherein the step of examining said data packet includes the further steps of:

checking header information of outbound data packets from said network stack to determine if processing applies; and

checking header information of inbound packets to said network stack to determine if said data packets include cryptographic functions.

5. An system for processing data packets by providing cryptographic functions to data packets at the PPP layer of a network stack, said system having:

a packet interceptor to intercept PPP datagrams inbound to said network stack and outbound of said stack, said PPP datagrams including at least one data packet, and to decapsulate said PPP datagrams to retrieve said encapsulated IP packet;

a security policy manager for storing processing rules for said data packets and selecting at least one of said processing rules for said data packet; and

a processing module for processing said data packet by selecting and applying said cryptographic transformations on said data packet, said processing module in communication with said security policy manager;

wherein PPP datagrams are intercepted in accordance with said processing rules.

6. The system of claim 5, wherein the packet interceptor is a software module located at the PPP layer of the network stack.

7. The system of claim 6, wherein said software module is a driver included in a kernel of an operating system in computer readable medium of said system.

8. The system of claim 5, wherein the cryptographic transformations are implemented using an IPsec protocol by said processing module.

9. The system of claim 5, wherein secure communications between correspondents is provided via a virtual private network.

10. An method for providing a cryptographic system for communication between correspondents in a communication network to data packets at the PPP layer of a network stack, said method having the step of:

providing a security module in a computer readable medium at each of said correspondents, said security module having:

a packet interceptor for intercepting PPP datagrams having at least one encapsulated data packet en route along the protocol stack and for decapsulating said PPP datagrams to retrieve said at least one encapsulated data packet,

a security policy manager for storing processing rules for said data packets and selecting at least one processing rules for said data packet; and

a processing module for processing said data packet by selecting and applying cryptographic functions to said data packet, said processing module in communication with said security policy manager;

examining said data packets outbound from said correspondent determine whether processing by said processing module is required; and

examining inbound data packets to said correspondent to determine whether processing by said processing module is required by checking whether said data packets include cryptographic functions.